Department of Homeland Security Daily Open Source Infrastructure Report for 07 February 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- WABC−TV reports thousands of commuters at the PATH station at New York's Exchange Place are being screened, scanned, and in some cases swiped for explosive residue similar to what is seen at airports, as a test case running three weeks. (See item 12)
- The Department of Homeland Security has launched Ready Kids, a family−friendly tool to help parents and teachers educate children about emergencies and how they can help their families better prepare. (See item 30)
- The Associated Press reports Italian officials have stepped up their security operations at the Turin Winter Olympics in response to worldwide protests among Muslims over caricatures of the Prophet Muhammad. (See item 37)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 05, Associated Press* — **High wind in Northwest cuts power.** Fierce wind across western Washington and Oregon on Saturday, February 4 cut power to homes and businesses, forced rail service and a major bridge to close, and was blamed for at least one death, authorities said. The wind raced through Seattle at 45 mph, with gusts higher than 50 mph, the

National Weather Service said. Gusts of more than 60 mph were recorded on the Olympic Peninsula, west of the city. Power was out for at least 160,000 customers in Washington and may not be restored for several days in the hardest hit areas, Puget Sound Energy spokesperson Lynn Carlson said. About 32,000 people lost power in Oregon, though crews had reduced the number to about 18,000 by early afternoon, Portland General Electric said. A ferry run connecting the Olympic Peninsula to an island in Puget Sound was shut down because of choppy waters. And Seattle's floating bridge, one of two routes linking the city with its eastern suburbs, was closed. A storm−related mudslide prompted a 48−hour shutdown of passenger rail service between Seattle and Vancouver, British Columbia. The closure affected Amtrak and commuter train service, said Gus Melonas, a spokesperson for Burlington Northern Santa Fe railroad.
Source: http://news.yahoo.com/s/ap/20060205/ap_on_re_us/washington_w inds_3

2. *February 05, Associated Press* — **China looks abroad for energy lifeline.** While striving to secure foreign oil and gas, China is struggling to limit soaring reliance on outside supplies by increasing nuclear and hydroelectric power. The voracious appetite for energy in China and other fast−developing nations, including India, is one factor propelling oil prices upward. Last year, China's state−controlled CNOOC Ltd. gave up an $18.5 billion takeover bid for Los Angeles−based oil company Unocal Corp. after critics complained the deal might jeopardize U.S. security. The energy buying spree has taken Chinese firms as far as Venezuela and Australia. In the past six months, these companies have signed deals totaling $7 billion for stakes in oil fields in Kazakhstan, Nigeria, and Syria. A state−controlled company is reportedly considering a $2 billion bid for another Kazakh property. "There is a strategic element to it," said Kevin Norrish, an energy analyst for Barclays Capital in London. "It's something that we've seen before. Japan was doing the same thing about 10 to 15 years ago, with a lot of its natural resource companies, including oil companies, buying into foreign projects."
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/02 /05/AR2006020500455_pf.html

3. *February 05, Pantagraph (IL)* — **Utilities plan for the worst.** Electric cooperative officials in Illinois have launched a massive review and update of a 25−year disaster plan they hope to complete by fall. "We've always had plans for major outages in which it would take three or four days to restore power. This plan will go two steps further. We are looking at how we will respond to something that probably won't happen, such as a major ice storm. And we want to be able to respond if our facility would be destroyed," said Jeff Reeves, Corn Belt Electric Energy Corporation chief executive officer. The organization is reviewing existing plans from other electrical cooperatives and lessons learned by Coast Electric Power Association. Corn Belt assisted Coast Electric with supplies and linemen when Hurricane Katrina left 70,000 Coast Electric customers powerless. Officials initially believed it would take six to eight weeks to restore power, but 10,000 visiting linemen from 22 states restored power in three weeks. Existing electrical cooperative disaster plans focus on assessing vulnerability to tornadoes, fire, floods, and earthquakes. The plans assess how long it might take to restore key business functions, establish an emergency response team, and develop a contact list of emergency providers and suppliers.
Source: http://www.pantagraph.com/articles/2006/02/05/business/10579 5.txt

4.

February 05, Idaho State Journal — **War games boost safety at nuke sites.** Department of Energy laboratory security teams travel the country mounting mock attacks on facilities and exposing any weaknesses. Idaho National Laboratory (INL) spokesperson John Walsh said, "That's the best way to find out how good we are and how good our systems are...Failure is not necessarily a bad thing. It can identify where we need work." In the mock attacks combatants are shadowed by controllers who monitor their actions. All movements and shots fired are recorded on a computer system and analyzed after each battle. Last year, INL security worker Neil Walker and his partner took fifth out of 42 teams at a sniper competition in Boise, ID. "We have a reputation. We went to that sniper school, and we [heard]'You got to watch out for those DOE snipers. They shoot long range,'" Walker said. INL's 280 security workers often train with the Butte County Sheriff's Office. The Special Response Team members train in heavy weapons and are equipped with night−vision helmets. Walker said "We try to make things as realistic as possible (in training)." They guard a self−contained city in the middle of nowhere. The 890−square−mile site has its own system of roads, sewers, water, power, and phone lines.
Source: http://www.journalnet.com/articles/2006/02/05/news/local/new s02.txt

5. *February 03, Global Security Newswire* — **Energy's radiation−detection center to respond to DHS needs, chief says.** A new Department of Energy (DOE) unit called the main U.S. radiation−detection laboratory will take some cues from a Department of Homeland Security (DHS) office set up last year, the director of the DOE project said this week. The Center for Radiation Detection Materials and Systems, part of the Oak Ridge National Laboratory, will seek to build on existing Oak Ridge strengths, Director Lynn Boatner said. The Tennessee center will develop new detection technology and will work to make new technology quickly deployable, he said, by agencies such as Homeland Security's year−old Domestic Nuclear Detection Office. "One of the things that we're emphasizing in this work is the rapid movement and transfer of new developments and new technology into systems −− fieldable systems for application in the field, for monitoring radiation in the areas in which [the center's consumers are] interested," he said. Post−September 11 worries about a radiological "dirty bomb" attack spurred the creation last year of the DHS detection unit, which the agency describes as "a single accountable organization ... to develop the global nuclear detection architecture and acquire and support the deployment of the domestic detection system." Last month, Oak Ridge announced the creation of its detection center.
Source: http://www.govexec.com/story_page.cfm?articleid=33305&dcn=to daysnews

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *February 06, United Press International* — **New Jersey plant leaks 4,000 gallons of oil.** State officials said there was no health hazard in central New Jersey after 4,000 gallons of fuel oil leaked from an asphalt plant into the Passaic River. An open valve on a 9,000−gallon above−ground tank at the Tilcon plant in Totowa, north of Newark, NJ, allowed the oil to leak into a catch basin, then through a sewer pipe into the river Sunday morning, said Totowa Police Chief Robert Coyle. State Department of Environmental Protection spokesperson Elaine Makatura said it has hired two contractors to work on containment, setting up booms, as well as onshore cleanup. A strong odor was evident along stretches of the river and near the leak site, but the spill does not present a danger to residents, and tap water is safe to drink, said state Rep.

William Pascrell (D−NJ). Monday, absorbent materials, floating booms and pumps to contain and remove the oil were still in place.
Source: http://www.postchronicle.com/news/breakingnews/article_21257 11.shtml

7. *February 06, Chicago Tribune* — **Residents are evacuated after gas line is broken in Chicago.** Workers broke a four−inch gas line in the 3500 block of North Narragansett Avenue Sunday, February 5, causing a local evacuation but no injuries, according to the Chicago Fire Department. Josh Dennis, department spokesperson, said it is unclear who broke the Peoples Energy line at about 2:20 p.m. CST. About 25 people were evacuated from their homes but returned after 3 p.m. CST when the leak was stopped, Dennis said.
Source: http://www.chicagotribune.com/news/local/chicago/chi−0602060 170feb06,1,3512405.story?coll=chi−newslocalchicago−hed

[Return to top]

Defense Industrial Base Sector

8. *February 06, Reuters* — **Bush proposes record $439.3 billion defense budget.** President George W. Bush on Monday, February 6, proposed a record $439.3 billion U.S. defense budget for 2007 aimed at fighting both unconventional terrorism and major conflicts with other nations if necessary. The Pentagon budget represented a 4.8 percent boost over current military spending as Bush seeks cuts in domestic programs. The Pentagon budget for the financial year beginning October 1 seeks $84.2 billion for weapons procurement, including additional unmanned aircraft to monitor threats by extremist groups and governments worldwide, and $73.2 billion for research and development on new arms. Both are increases from fiscal 2006. The defense budget also would boost Army spending to $111.8 billion next year, a major increase over the current $99.2 billion, to repair and modernize a service that has been strained by the Iraq and Afghan wars. The proposed Pentagon budget is only a part of the national defense picture and does not include $120 billion in planned new U.S. funding for military and other operations in Iraq and Afghanistan. That money is included in separate legislation.
Source: http://today.reuters.com/news/newsArticle.aspx?type=politics News&storyID=2006−02−06T163005Z_01_N06395806_RTRUKOC_0_US−MZ −BUSH−BUDGET−DEFENSE.xml&src=cms

9. *February 02, Federal Computer Week* — **Marines terminate Accenture contract.** The Marine Corps has terminated a six−month, $4.5 million contract awarded to Accenture last summer to design and implement its new global supply chain and maintenance system. The Marines canceled Accenture's contract on the Global Combat Support System−Marine Corps because the company did not meet the contract's requirements, terms and conditions, said Capt. Jeff Landis, a spokesperson at the Marine Corps Systems Command at Quantico, VA. He confirmed the contract termination Thursday, February 2, and read parts of the termination−for−cause letter. Accenture failed to deliver substantial documentation in support of the system's detailed design review. The company also did not comply with cost, schedule and performance baselines and risk assessments for the next phase of the program, Landis said. Landis said the Marines plan to recompete the contract, but he did not provide a date for the release of the new solicitation.
Source: http://www.fcw.com/article92191−02−02−06−Web

[Return to top]

Banking and Finance Sector

10. *February 06, Federal Trade Commission* — **Agencies in U.S. and Canada promote education, awareness, and partnerships during National Consumer Protection Week 2006.** The Federal Trade Commission (FTC) has launched the eighth annual National Consumer Protection Week (NCPW), February 5−11, 2006, in cooperation with federal, state, and local agencies, and national advocacy organizations committed to consumer protection and education. At the Canadian Embassy, the FTC, with the United States Postal Inspection Service, the Postal Service's Consumer Advocate, the Royal Canadian Mounted Police, PhoneBusters, and Canada's Competition Bureau announced their commitment to combat cross−border fraud as part of NCPW. The FTC also unveiled the "Grand Scam Challenge," online, interactive games that teach consumers about topics such as identity theft, the National Do Not Call Registry, and spam. The "Grand Scam Challenge" is an innovative, entertaining way for consumers to learn about common scams and get valuable information playing three new, online games. In the games, players are directed to the FTC's Website for more information about the topics, including: scholarship Scams, bankruptcy, identity theft, credit, phishing, Internet auctions, among other topics. The FTC enters Internet, telemarketing, identity theft, and other fraud−related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.
    Grand Slam Website: http://www.consumer.gov/ncpw.
    FTC Website: http://www.ftc.gov
    Source: http://www.ftc.gov/opa/2006/02/ncpw.htm

11. *February 05, Canadian Press* — **Data on Americans faxed to Canadian company.** Confidential information on hundreds of United States citizens, including social security numbers, health information and bank account numbers, is being sent mistakenly by fax to a small Manitoba company North Regent Rx, an herbal remedy distribution company. "I know how much these people make, I know what their social security number is, I know where they live...Almost everything a person needs for identity theft is actually faxed to us on a daily basis," North Regent Rx spokesperson Jody Baxmeyer said. Baxmeyer says his company has been trying to stop the faxes from coming in, but has been unable to reach an agreement with Prudential Financial, the U.S.−based company that is the intended recipient. The problem started as soon as North Regent Rx began operating 15 months ago, when employees at doctors' offices began faxing medical benefits to Prudential's insurance division, but mistakenly dialed the fax number of North Regent Rx, which is very similar. The data reveals information about people in many states. Another instance of information submitted improperly occurred between 2001 and 2004, when confidential information about hundreds of Canadian Imperial Bank of Commerce customers was faxed to a scrapyard in West Virginia.
    Source: http://cnews.canoe.ca/CNEWS/Canada/2006/02/05/pf−1427234.htm l

[Return to top]

Transportation and Border Security Sector

12. *February 06, WABC−TV (NY)* — **Airport−style security begins at PATH stations.** Beginning Monday, February 6, thousands of commuters are being screened, scanned, and in some cases swiped for explosive residue. The Department of Homeland security is turning the PATH (Port Authority Trans−Hudson) station at Exchange Place into a test case. The Port Authority says the screening will add one minute to a commute, but for the 15,000 riders who use the PATH station at Exchange Place this is all voluntary. The screening will be similar to what is seen at airports since 9/11. This screening is a ten million dollar test program running just three weeks. The U.S. Department of Homeland Security needs real−world data to develop the technology to screen for explosives at a distance. That's become a priority since the Madrid bombings in 2004 and last summer's subway attack in London.
Source: http://abclocal.go.com/wabc/story?section=traffic&id=3879842

13. *February 06, New York Times* — **Indicting boat's captain, U.S. sends a message.** The 38−foot charter vessel Sydney Mae II sunk last September off Oregon's coast, throwing the captain and four other people into the icy surf after a long day of tuna fishing. Three people died, and two were rescued, including the captain. In mid−January, the Justice Department invoked a rarely used 154−year−old statute and indicted the skipper of the Sydney Mae II, Richard J. Oba, on three counts of seaman's manslaughter. Federal officials said Oba, 58, a captain with 30 years of experience, acted negligently by repeatedly ignoring warnings from the Coast Guard to back away from an area that was being hammered by high swells. The sinking of the Sydney Mae II is being used by the federal authorities to send a message to thousands of boat operators that they can face years in prison if people die while on board a ship under their command. Meanwhile, federal officials are still investigating the cause of another accident that has prompted calls for tighter regulation of commercial boating, the capsizing of a tour boat last October on Lake George in New York, where 20 elderly tourists died.
Source: http://www.nytimes.com/2006/02/06/national/06shipwreck.html?_r=1&pagewanted=all&oref=slogin

14. *February 06, Associated Press* — **Arizona state police should stem flow of migrants, lawmakers say.** Lawmakers are considering an aggressive approach for trying to lessen Arizona's role as the busiest gateway for sneaking into the country: devoting squads of the state police to catch illegal immigrants who slip past federal border agents. Over the years, many officials have resisted suggestions for local and state police agencies to confront illegal immigration, long considered the sole province of the federal government. But the notion is gaining political traction as the public's frustration with the state's porous border with Mexico grows. A state lawmaker has proposed a plan that includes $20 million for the Arizona Department of Public Safety to run a 100−member squad to operate surveillance equipment, construct border barriers, target drug and immigrant smugglers and perhaps patrol the border. A different plan by Governor Janet Napolitano would include two state police squads to focus on immigrant smuggling cases and, like the other proposal, would provide money for combating gang−related border crime. Both plans also would offer millions of dollars to communities to tackle illegal immigration. Public pressure is mounting for state politicians who face re−election races this year to confront illegal immigration in Arizona, a hub for smugglers who transport immigrants across the country.
Source: http://www.tucsoncitizen.com/news/local/020606a2_BorderPolic e

15. *February 06, Reuters* — **JetBlue loses some luster.** The No. 2 U.S. discount airline shocked investors and analysts on Wednesday, February 1, by disclosing that not only had it posted its first quarterly loss since going public in April 2002 but that it expected to stay mired in the red for the rest of 2006. Even the leather seats, seat−back satellite televisions and cheerful personnel that made the carrier a hit with passengers have lost a bit of luster as JetBlue has struggled with one of the industry's worst on time performances. The airline faces several problems: the soaring cost of fuel, a breakneck expansion that includes the addition of a second aircraft type, and tough competition that has loomed as an obstacle to fare hikes in key markets. Also, analysts are questioning the airline's failure to buy contracts that could have softened the blow of soaring oil prices. "They should have known to lock in hedges and they really didn't effectively do so," said Jim Corridore, an equity analyst at Standard & Poor's.
Source: http://biz.yahoo.com/rb/060202/airlines_jetblue.html?.v=1

16. *February 06, Department of Transportation* — **Secretary Mineta announces budget for FY 2007.** Department of Transportation Secretary Norman Y. Mineta on Monday, February 6, unveiled a $65.6 billion Fiscal Year 2007 budget request that provides record investments for new highway, transit and safety programs, explores new ways to fund transportation projects over the long term, and provides funds to encourage continued Amtrak reform. The budget fully funds the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users at nearly $50 billion for transit, highways and safety programs, a $3.3 billion increase over 2006. The Administration’s proposal includes $900 million for Amtrak. Of that, $500 million is for capital needs and maintenance, especially along the Northeast Corridor where Amtrak owns most of the tracks. The remaining $400 million will fund Efficiency Incentive Grants to encourage reforms of the railroad service, Mineta added. The budget requests $13.7 billion for the Federal Aviation Administration, including $8.4 billion to address operational needs, hire 194 inspectors and other safety personnel and 1,136 new air traffic controllers to offset retirements expected in 2007. It also provides $2.8 billion for the Airport Improvement Program to construct new runways.
A detailed Budget in Brief soon will be available at http://www.dot.gov
Source: http://www.dot.gov/affairs/dot2106.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

17. *February 05, Monitor (TX)* — **Agencies, citizens join to fight citrus disease.** Citrus greening disease’s possible threat to Texas' Rio Grande Valley’s citrus industry has spurred a collaborative effort at the federal, state, and local levels to gather help from local residents in spotting the ailment. The Texas Cooperative Extension, together with Texas A&M University−Kingsville’s Citrus Center, has recruited about two dozen people −− including 14 seasonal visitors, several full−time Valley residents and even the regional urban forester −− to

survey voluntarily trees and fruit in RV parks and in private back yards until December. State and U.S Department of Agriculture officials will also inspect commercial citrus groves and nurseries for citrus greening. While the disease is not yet in the Valley, the insect that carries the disease −− the Asian citrus psyllid −− has been in the area since 2001. Citrus greening disease is "a death sentence for trees" because it lies dormant for up to three years and destroys not only the plant but the fruit as well, said Florida Department of Agriculture spokesperson Denise Feiber. The disease hit several Florida crops in September 2005. As of January 10, 558 trees are confirmed positive for citrus greening.
Source: http://www.themonitor.com/SiteProcessor.cfm?Template=/GlobalTemplates/Details.cfm&StoryID=11406&Section=Valley

18. *February 03, Purdue University* — **Gene thwarts some pathogens, gives access to others.** A Purdue University plant biologist and his collaborators in Austria and North Carolina identified the gene that helps plants recognize pathogens and also triggers a defense against disease. The gene and its defense mechanisms are similar to an immunity pathway found in people and in the laboratory research insect, the fruit fly. As Botrytis cinerea, a pathogen that makes strawberries gray and fuzzy, tries to invade a plant, the gene BIK1 recognizes the pathogen and sets off a defensive reaction. Another type of pathogen, called a biotroph, must feed on live plant cells. As a strategy to contain a pathogen, plants actually kill their own cells at the site where a biotrophic pathogen is attempting to invade. "This gene, BIK1, makes plants resistant to pathogens such as Botrytis, but it allows biotrophic pathogens to invade," said Tesfaye Mengiste, a Purdue plant molecular biologist. "The mutant plant that doesn't have BIK1 actually shows decreased immunity to two pathogens, including Botrytis. But unexpectedly, it is completely resistant to virulent strains of the biotrophic bacteria." The disease caused by Botrytis destroys about 10 percent of the grape crop annually and about 25 percent to 30 percent of tomato and strawberry crops in some seasons.
Source: http://news.uns.purdue.edu/UNS/html4ever/2006/060203.Mengist e.bik1.html

19. *February 03, Bloomberg* — **Texas cattlemen watch as drought, wildfires destroy pastures.** Drought conditions across Texas, the largest U.S. cattle−raising state, have parched pastures. Wildfires have destroyed much of the vegetation north of Dallas, adding to the woes of an industry with more than six billion dollars in annual sales in the state. Ranchers have responded by selling more cattle than usual for this time of year. There were four percent more cattle in feedlots on January 1 than a year earlier, according to the U.S. Agriculture Department. The increase in Texas, home to 25 percent of the cattle in feedlots, was twice that amount. Ranchers typically put seven−month−old calves out to graze until they grow to about 700 pounds. The cattle are sold to feedlots, where they are fattened to 1,200 pounds over five months before being sent to slaughterhouses. The area with the worst drought starts north of Dallas, extends southwest through Austin, and reaches the southwestern part of the state. The region scores from 600 to 800 on an index used by the Texas Forest Service, with 800 being the most extreme drought conditions. Texas Governor Rick Perry declared a statewide drought disaster on January 19 and requested federal disaster relief for farms and ranches across the state's 254 counties.
Source: http://www.bloomberg.com/apps/news?pid=10000103&sid=a4lDRqO1YmlM&refer=us

[Return to top]

Food Sector

20. *February 06, Deutsche Presse−Agentur* — **U.S. beef to return to Taiwan.** U.S. beef will return to Taiwan on Thursday, February 9, after Taipei conditionally lifted a seven−month ban imposed due to fears over mad cow disease, the Central News Agency said on Monday, February 6. The first shipment of U.S. beef will arrive at the Chiang Kai−shek International Airport outside Taipei on Thursday. On Friday, February 10, Department of Health Director Hou Sheng−mao will go to the CKS airport to inspect the import procedure of U.S. beef. Taiwan banned U.S. beef imports in December 2003 following reports of the first U.S. mad cow case, but lifted the ban on April 16, 2005. Taiwan banned U.S. beef imports again on June 25, 2005 after a second case of the disease was confirmed. On January 25, Taiwan announced a conditional resumption of U.S. beef imports.
Source: http://news.monstersandcritics.com/business/article_1095163.php/US_beef_to_return_to_Taiwan_on_Thursday_report

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

21. *February 06, Agence France−Presse* — **Iraq confirms second death in bird flu alert.** A second Iraqi Kurd was confirmed to have died from the H5N1 bird flu strain as international teams arrived to combat the spread of the virus in the country's north. Hamma Sur Abdallah, 40, who died of flu−like symptoms a little over a week after his niece passed away under similar circumstances, was confirmed as having died of virus by a lab in Cairo, Egypt, a senior Kurdish health official told Agence France−Presse. A few days after Abdallah's death, the World Health Organization (WHO) lab confirmed his niece Shajin Abdel Qader had died of bird flu. On Monday, February 6, the WHO said there were seven more suspected cases of bird flu in Iraqi Kurdistan. Further tests are underway in Britain on virus samples from Abdallah, as well as on samples from a woman who comes from the same region and remains in hospital. Meanwhile, a large consignment of masks, gloves and gowns is on its way from the U.S. to help the war−torn country fight a deadly outbreak. The WHO said it was dispatching thousands of doses of the anti−influenza drug Tamiflu after reports of an acute shortage.
Source: http://news.yahoo.com/s/afp/20060206/wl_mideast_afp/healthfluiraq_060206161442;_ylt=Al9LPyD_fnT6Ay1JVhTW_AXuOrgF;_ylu=X3oDMTA2ZGZwam4yBHNlYwNmYw−−

22. *February 06, Government Computer News* — **Health IT leaders set an aggressive schedule.** Several small−scale tests of health IT over the next year should go a long way toward showing physicians and consumers the possibilities of fusing technology and health care. The public−private American Health Information Community (AHIC) −− led by Health and Human

Services Department (HHS) secretary Michael Leavitt—is fleshing out plans for the first version of personal health records and other health IT initiatives on an aggressive schedule. Pilots are expected by December 31. The first versions will test small components using existing technologies that will later become part of comprehensive systems. On its Website, the White House lists projects for this year, including the "medical clipboard," medication history, lab results, and disease monitoring tools. AHIC has developed a road map for its early versions of a personal health record, bioterrorism response, electronic health record and online tools to help streamline chronic care by December. AHIC workgroups are made up of representatives from federal and state government, health care providers and payers, and the IT industry. AHIC also will incorporate work by vendors and groups that HHS has contracted to develop and test electronic prescribing, interoperability standards, product certification, and prototypes for a nationwide health information architecture.
Source: http://www.gcn.com/25_3/news/38187−1.html

23. *February 06, New York Times* — **States and cities lag in bird flu readiness.** The nation's 5,000 state and local health departments are rushing to plan for an epidemic of avian flu, but they say they are hobbled by a lack of money and guidance from the federal government. Only a few places, particularly Seattle, WA, and New York City, have made significant progress, experts say. Most departments say they expect to be unprepared for at least a year. Under the response plan issued by the Bush administration the federal government has primary responsibility for creating stockpiles of vaccines and antiviral drugs, but the states and local governments are responsible for quarantines, delivering vaccinations and assuring that the sick get medical care. Even if a vaccine were available, few communities would be prepared to dispense it quickly. There are few local stockpiles of masks and hand sanitizers, and none of expensive equipment, like ventilators. The biggest danger, public health officials said, is the one over which they have the least control: hospitals in their regions, most of which are privately owned, cannot handle big surges of patients. Roger P. Baxter, head of flu preparedness for Kaiser Permanente, said his California hospital network was "probably better off than 90 percent of the health systems out there, and we have no surge capacity."
Source: http://www.nytimes.com/2006/02/06/politics/06flu.html?_r=1&hp&ex=1139202000&en=236fe0dc959ce159&ei=5094&partner=homepage &oref=slogin

24. *February 06, Agence France−Presse* — **U.S., French health agencies join forces to detect bird flu.** France and the U.S. are to join forces to detect early outbreaks of bird flu under an agreement signed in Paris, France, officials from both countries said in a joint statement. The memorandum of understanding struck between France's Pasteur Institute and the U.S. Department of Health and Human Services said they "agreed to carry out joint activities, beginning in Southeast Asia, to strengthen global capacity to detect influenza viruses that could have the potential to trigger a human pandemic." The H5N1 strain of the virus has claimed more than 85 human lives, most of them in Asia, though fears that it could mutate into a devastating form transmitted between humans have not yet been realized. The Franco−U.S. agreement establishes a joint working group that aims to increase H5N1 testing in at−risk countries and provide public awareness campaigns.
Source: http://news.yahoo.com/s/afp/20060206/hl_afp/healthflufranceus_060206161851;_ylt=Ans.ETXA.xHD8UnlyNa7lb.bOrgF;_ylu=X3oDMTA2ZGZwam4yBHNlYwNmYw−−

25. *February 05, Agence France−Presse* — **Eleven more suspected Indonesian bird flu cases await confirmation.** Indonesia, which has already registered 16 bird flu deaths, is awaiting test results from the World Health Organization (WHO) on 11 more suspected infections. "The latest report we have shows that there has been a total of 23 cases of confirmed infection, 16 of them fatal, while we are still awaiting the result of WHO tests on 11 other probable cases, four of them fatal," said an official at the health ministry's bird flu information center. The official, who identified himself as Nurdin, said local tests on the 11 probable cases had tested positive but that only tests conducted by the WHO laboratory in Hong Kong would officially confirm infection cases. "But from experience, the WHO tests have only confirmed the results of our tests," Nurdin said. A WHO team warned last month that Indonesia needed to focus more on measures aimed at preventing virus transmission and also on preparations for a possible human pandemic. Experts fear that H5N1 could mutate into a form easily transmissible by humans, sparking a global pandemic.
Source: http://news.yahoo.com/s/afp/20060205/wl_asia_afp/healthfluindonesia_060205055614;_ylt=Ap4v9r5Scv00ilkEuRayHKKJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *February 05, Catoosa County News (GA)* — **Georgia county simulates Category 4 hurricane disaster.** Catoosa County, GA, leaders and emergency personnel took part in a simulated disaster Saturday, February 4, the culmination of a three−week training program to prepare for emergency situations. Graduates participated in the mock drill at the Colonnade and utilized the National Incident Management System's Incident Command System method to control the situation. The scenario involved Catoosa County being hit by Bubba, a Category 4 hurricane. For the past three weeks local law enforcement officers, firefighters, city and county officials, emergency medical services personnel and more have been learning about the systematic and specific approach for dealing with emergencies. In the hurricane scenario Saturday, participants learned of developing situations about every 30 minutes and had to strategize and decide how to implement emergency services. Participants were divided up into two groups of ten and pretended to be working a command station. They were put into new roles aside from what they normally do, but roles they could fill in the event of an emergency. The groups' job was to outline the incident plan and identify resources. The biggest benefit of the mock drill was that it gave a variety of people the opportunity to actively participate in an emergency command situation.
Source: http://news.mywebpal.com/news_tool_v2.cfm?show=localnews&pnpID=724&NewsID=694734&CategoryID=3418&on=1

27. *February 05, Miami Herald (FL)* — **First responders to get technological upgrade.** City

Council members in Plantation, FL, recently approved a $2 million contract to install laptop computers and software in police and fire vehicles. "This is going to bring us up to speed with the current technology," Plantation Fire Battalion Chief Joel Gordon said. Currently, dispatchers rely on squawky radios to transmit information about locations and details of 911 calls. And when police officers need to run a license plate through a database to check for outstanding warrants, they must wait until a dispatcher is free to do the check. With the new technology, all the pertinent information will pop up on a map on the laptop's screen. Indicators will show where every emergency vehicle is so workers know their location to an emergency relative to other first responders. The software will show emergency workers where there are roadblocks and suggest an alternate route. Officers will be able to run license checks themselves on the computers. In addition, firefighters will know before they arrive at a fire whether the building has any code issues or has had failed inspections. And they will know where the nearest fire hydrant is and where nearby gas and water lines are located.
Source: http://www.miami.com/mld/miamiherald/news/local/states/florida/counties/broward_county/cities_neighborhoods/plantation_s unrise/13788541.htm

28. *February 04, Pine Bluff Commercial (AR)* — **Arkansas' chemical stockpile program to conduct emergency exercise.** The Pine Bluff Arsenal and the Chemical Stockpile Emergency Preparedness Program (CSEPP) will be conducting an exercise Wednesday, February 8, to simulate an emergency scenario involving chemical weapons at the arsenal. Wayne Norton, public information officer for the Jefferson County Office of Emergency Management (OEM), said sirens and tone−alert radios will be sounded with an exercise message in the affected zones during the exercise. Participants will not know which zones will be included in the three−hour exercise until that day, he said, but off−post soundings are expected. “[The sirens] are initially sounded by the arsenal as they would be in the case of a real event,” Norton said. “The Jefferson County OEM will then issue two additional soundings in the affected zones only in 12−minute intervals.” Tone alert radios will be set off by the Arsenal with an exercise message in the affected zones. “This is a federally−mandated exercise,” said Carole Newton, CSEPP public affairs officer. “The Federal Emergency Management Agency and the Army use the exercise each year to assess the preparedness of all the chemical weapons storage sites.” An estimated 200 to 300 responders, evaluators, observers and controllers will be on hand.
Source: http://www.pbcommercial.com/articles/2006/02/05/news/news4.t xt

29. *February 04, Contra Costa Times (CA)* — **California city's emergency radio plan receiving criticism.** A planned $1.4 million upgrade of Oakland, CA's, emergency radio system is drawing criticism from officials who say it could drive the city away from a unified East Bay communications network and complicate outside efforts to help the region in the event of a major disaster. The discord surrounds a proposal to buy two new antennas that would boost the transmission power of Oakland's emergency radios. The City Council will be asked Tuesday, February 7, to approve the purchase. Critics say the investment would signal Oakland's further commitment to an outdated system that is incompatible with much of the rest of the East Bay and run counter to plans for Contra Costa and Alameda counties to build a new, regional radio network that would let firefighters, police and other emergency workers talk to each other. City officials say the new antennas would be a temporary fix to overcome dead spots that plague police and fire officials in certain parts of the city and should not be viewed as a step away from a regional communications system in the future.
Source: http://www.contracostatimes.com/mld/cctimes/news/politics/13 791558.htm

30. *February 02, Department of Homeland Security* — **DHS launches Ready Kids.** The Department of Homeland Security (DHS) and the Advertising Council Thursday, February 2, launched Ready Kids, a family−friendly tool to help parents and teachers educate children, ages 8−12, about emergencies and how they can help their families better prepare. The Ready Kids program launched at Andrew Jackson Language Academy in Chicago with a roundtable discussion led by DHS Secretary Michael Chertoff and an interactive presentation for families by local first responders. Ready Kids is the newest addition to the successful Ready campaign, a national public service advertising campaign designed to educate and empower Americans to prepare for and respond to emergencies, including natural disasters and potential terrorist attacks. Secretary Chertoff said, "We hope the Ready Kids Website and in−school materials will help facilitate discussions about this important subject and encourage all families to get an emergency supply kit, make a family emergency plan and be informed about the different emergencies that can happen."
Ready Kids fact sheet: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0847.xml
Ready Kids Website: http://www.ready.gov/kids/home.html
Source: http://www.dhs.gov/dhspublic/display?content=5383

[Return to top]

Information Technology and Telecommunications Sector

31. *February 06, Computer World* — **Microsoft and Washington state sue spyware company.** Microsoft and the Washington state attorney general have filed lawsuits against antispyware software vendor Secure Computer, alleging that the company's Spyware Cleaner software not only fails to remove spyware as advertised, but makes changes to users' computers that make them less secure. The attorney general's lawsuit is the state's first to be filed under Washington's 2005 Computer Spyware Act. Washington's 16−count lawsuit was filed in U.S. District Court in Seattle and follows investigations by both Microsoft and the Attorney General's high tech fraud unit. The state's lawsuit also names Secure Computer president Paul Burke and Web domain owner Gary Preston, both of New York state, as defendants. It further charges Zhijian Chen, of Portland, OR; Seth Traub, of Portsmouth, NH; and Manoj Kumar, of Maharashtra, India, in connection with the advertising of the product. Microsoft has also sued Secure Computer, alleging that the company's Spyware Cleaner e−mail and pop−up advertisements falsely suggested that Microsoft endorsed the product, says Nancy Anderson, vice president and deputy general counsel with Microsoft.
Source: http://computerworld.co.nz/news.nsf/scrt/F03EF851B098CED6CC2 5710900776B50

32. *February 06, Computer World* — **China attacks UK Parliament using Windows security hole.** Chinese hackers attacked the UK Parliament in January, the government's e−mail filtering company, MessageLabs, has confirmed. The attack, which occurred on January 2, attempted to exploit the Windows Meta File (WMF) vulnerability to hijack the PCs of more than 70 named individuals. E−mails were sent to staff with an attachment that contained the WMF−exploiting Setabortproc Trojan. Anyone opening this attachment would have enabled attackers to browse files and possibly install a key−logging program to attempt the theft of passwords. None of the e−mails got through to the intended targets, MessageLabs says, but the

UK authorities were alerted. MessageLabs said the e−mails had been traced to servers in China's Guangdong Province, hence the suspicion that the latest attack was part of a more general campaign of electronic subversion. This is not the first time the UK Government has come under Trojan attack from China. Last summer, the National Infrastructure Security Coordination Center (NISCC) reported that UK government departments had been hit by a wave of Trojans originating in China.
Source: http://computerworld.co.nz/news.nsf/scrt/AFAC1C3187BF9027CC2 5710900773FD8

33. *February 03, Tech Web* — **Report: ISP filters forcing decline in spam.** ISP filters are largely responsible for a decline in e−mail spam, which is expected to continue declining through 2010, according to a report released Friday, February 3, by Jupiter Research. Jupiter said the average e−mail consumer received 3,253 spams in 2005, but that number will drop to 1,640 in 2010. The company forecasts that the volume of spam messages per consumer will decrease by 13 percent a year until 2010. "The next five years will see a more organized e−mail marketing arena," said David Schatsky, senior vice president of research, in a statement.
Source: http://www.techweb.com/wire/security/178601917;jsessionid=5S PNDZX55YKH4QSNDBOCKHSCJUMEKJVN

34. *February 03, Associated Press* — **Experts: Hype may have mitigated Kama Sutra worm.** Companies and individuals heeded this week's warning about a file−destroying computer worm known as "Kama Sutra," helping minimize its damage Friday, February 3, security experts said. One Italian city shut down its computers as a precaution, but otherwise the worm's trigger date arrived with relatively few reports of problems. Hundreds of thousands of computers were believed to be infected, but security vendors say many companies and individuals had time to clean up their machines following the alarm, carried by scores of media outlets. "The importance of media attention from an awareness and educational standpoint has been a very good thing," said Marc Solomon, director of product management at security vendor management McAfee Inc. "It alerts users to what may have happened and the destruction that could have occurred." David A. Milman, chief executive of the Syracuse, NY−based Rescuecom, said, "the hype was probably what prevented the disaster from happening."
Source: http://wireservice.wired.com/wired/story.asp?section=Technol ogy&storyId=1154343

35. *February 03, Newsfactor Magazine Online* — **WMF exploits sold by Russian hackers.** According to Moscow−based antivirus firm Kaspersky Labs, Russian hackers propagated the Windows Meta File (WMF) exploit that wreaked so much havoc on computers in December 2005 by selling it to Internet criminals for $4,000. The exploit took advantage of a bug in Windows' rendering of WMF images, putting PC users at risk when they visited Websites that had been infected by the exploit. In a posting on its Website, Kaspersky said that over a thousand instances of malicious code based on the exploit were detected in a week. But because of the Christmas holiday season, less damage occurred than might have happened otherwise, Kaspersky said. According to Kaspersky researchers, the person who discovered the exploit in early December began selling it by the middle of that month to anyone prepared to pay $4,000. But the antivirus community only identified the exploit on December 27.
Source: http://www.newsfactor.com/news/WMF−Exploits−Sold−by−Russian− Hackers/story.xhtml?story_id=01200162XEHO

36.

February 03, Reuters — **Hackers tap Greek government cell phones.** Unknown eavesdroppers tapped the cell phones of Greek Prime Minister Costas Karamanlis, five cabinet members and dozens of top officials for about a year, the Greek government said on Thursday, February 2. Illegal software installed at Greece's second biggest mobile phone operator, Vodafone Greece, allowed calls to and from about 100 phones to be recorded. Most belonged to the government but one was owned by the U.S. embassy in Athens, officials said. "The phones tapped included the prime minister's, the whole leadership of the defense ministry and the whole leadership of the public order ministry, some foreign ministry phones, one former minister, now in opposition, and others," government spokesperson Theodore Roussopoulos told a news conference. The wiretaps lasted from just months before the 2004 Athens Olympics until March 2005, when Vodafone Greece discovered the incident. "As soon as we discovered the phone−tapping software, we removed it and informed the state, as was our obligation," George Koronias, head of Vodafone Greece, said in a statement. But the shutdown of the illegal software in the Vodafone system wiped out all traces of how and from where it had been installed, Public Order Minister George Voulgarakis told the news conference.
Source: http://news.zdnet.com/2100−1009_22−6034895.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT continues to contact and receive reports from federal agencies that have been affected by the CME−24 virus. The CME−24 worm actively disables anti−virus software on a host system and will also overwrite users' data files on the third of every month. This virus affects all recent versions of Microsoft Windows.

The CME−24 worm spreads primarily by harvesting email addresses from files on the local machine and then emailing itself as an executable attachment. It uses subject lines such as "Photos", "*Hot Movie*", and "Miss Lebanon 2006" to entice the user into opening the attachment. As soon as the attachment is executed, the user's system is immediately infected. Infected hosts within a network enclave will also try to spread locally through network shares with weak passwords.

On the third of every month, CME 24 will over write users' files on all accessible drives with the message "DATA Error [47 0f 94 93 F4 F5]". This will happen approximately 30 minutes after the user logins to the infected machine. The files affected by this variant will have the following file extensions: .doc, .xls, .mdb, .md3, .ppt, .pps, .zip, rar, .pdf, .psd, and .dmp.

Agencies that observe communication from internal machines to the 207.172.16.155 address should investigate further to determine if these machines are infected. Several agencies have reported that the systems that were impacted had anti−virus

but were not running the latest signatures.

US−CERT recommend the following course of action:

Ensure that the latest anti−virus definitions are loaded on servers and workstations.

Leverage Internet Content Filtering Solutions to block executable and unknown file types at the email gateway

Setting up an access control list to detect users from browsing to the aforementioned websites/IP addresses. LURHQ provides snort signatures related to the CME−24 worm on their website.

Monitoring of outbound traffic to identify potential malicious traffic or information leaks.

The infected host will also access a website with a web counter. This web counter shows how many machines have been infected, although it is expected that an infected machine may access the website on multiple occasions, thus inflating the number. The original web counter showed consistent growth with over 500,000 infections on Saturday and is now currently showing over 700,000 infections. However, recent web log postings suggest that the number is much closer to 300,000 unique addresses. FBI agents have received log data that resided on the web server, and is sharing the bulk data with US−CERT for analysis.

Please report any validated agency connection to the 207.172.16.155 website during the last 30 days to the US−CERT for further correlation and analysis.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4556 (−−−), 6346 (gnutella−svc), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 139 (netbios−ssn), 50497 (−−−), 32768 (HackersParadise), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

37. *February 06, Associated Press* — **Italians increase security for Olympics.** Security officials at the Turin Winter Olympics have stepped up their efforts in response to worldwide protests among Muslims over caricatures of the Prophet Muhammad. Italy's top law enforcement agencies met on Monday, February 6, with Interior Minister Giuseppe Pisanu, who was briefed by Italy's intelligence agency Sisde on the measures under way at the Olympics, a statement from his office said. "Particular attention was dedicated to the consequences that there could be

in Italy from the wave of protests in the Islamic world and to the additional prevention measures adopted in recent days," the statement said. Italy is mounting a massive security operation in Turin, with some 10,000 police reinforced by soldiers to protect Olympic venues. NATO is providing two AWACS surveillance planes to patrol over northern Italy during the Games, which begin Friday, February 10 and end February 26. Monday's briefing was also prompted by protests that enveloped the Olympic torch relay Sunday, February 5, as it passed through a northern valley recently wracked by violent demonstrations against the construction of a high−speed rail line. Torch bearers were forced to change their route after it was surrounded by demonstrators who unsuccessfully tried to extinguish the flame with a banner. Source: http://www.phillyburbs.com/pb−dyn/news/48−02062006−608961.ht ml

[Return to top]

General Sector

Nothing to report.
[Return to top]